

ENQPY™

S E C U R I T Y , S E T T L E D . ™

Cryptography took the wrong turn seventy-seven years ago. Every cipher built since is broken — in time, by computational advance, instantly by future platforms. **The world has been sold a bill of goods.**

Medical records encrypted today are being stolen and stored, waiting for the quantum computer that will read them. Banking communications, diplomatic cables, voting systems, critical infrastructure, personal messages, corporate secrets — all protected by ciphers with mathematical expiration dates. Post-quantum standards are heavier, slower, still breakable in principle. The treadmill never stops. Six trillion dollars a year in cybercrime is the bill being paid for cryptography that chose *hard enough* over *provably secure*.

In 1949 Claude Shannon defined the only cipher he considered ideal: one that leaves the adversary without a correct answer, no matter how much ciphertext is intercepted. The One-Time Pad satisfies it but requires a key as long as every message — practically useless. Shannon then introduced a second method: a finite-key cipher with the same permanent-uncertainty outcome. He thought constructing it was too difficult. **He walked away. Cryptography walked away with him.** Seventy-seven years of progress happened avoiding the problem — not working on it.

In March 2026, after thirty years, Paul McGough took up the problem Shannon had abandoned — and proved it. Enqpy™ is the first finite-key cipher with a formal proof that the message stays hidden from ciphertext alone — for any quantity of ciphertext, against any adversary including quantum, forever — derived from algebra, not from a hard problem. From ciphertext alone, the security is not *hard* to break. It is **mathematically impossible** to break. McGough named it what it is: **Absolute Secrecy**. Provable. Practical. Permanent.

Gil Vernam built the cipher. Claude Shannon introduced the theory.

Paul McGough proved the practice.

The question of whether digital secrets can be kept, is no longer open. A finite key, on any device — phone, chipset, satellite, pacemaker, voting machine — produces ciphertext that no adversary, of any power, at any point in the future, can read from the ciphertext alone. The harvest-now-decrypt-later threat disappears. The quantum cliff disappears. The upgrade cycle from RSA to ECC to post-quantum to the-next-thing ends. Not an incremental improvement — the destination, reached.

McGough is an engineer and inventor, not a credentialed academic cryptographer. He spent three decades on one problem because he was not answering to a tenure committee, a quarterly return, or an advisor's timeline — he worked until it was true and he could prove it. The underlying primitives received a formal cryptographic assessment by Dr. Giovanni Di Crescenzo at Telcordia in 2011 (zero exposures; all requirements rated 8 or 9 of 10), and were presented by Di Crescenzo and Glenn Veach at the 2015 NIST Lightweight Cryptography Workshop — the forum that initiated the effort now producing NIST's post-quantum standards. A prior entity, Qwyit LLC, was sold to HST Global Inc. in March 2025; NQP LLC holds the post-closing innovations.

The public release is deliberate. The proof is published in the public record at enqpy.com, with permanent archival deposits. The C reference is on GitHub at github.com/nqp-llc/enqpy. Enqpy™ is not for sale — and it is not being given away. McGough holds the patents, and has bound them open: a dated, irrevocable, successor-binding covenant never to assert them against the world's use of the cipher. He kept ownership so the openness could be guaranteed and verified — a public promise that cannot be taken back. Enqpy™ Foundation Inc. — filed April 2026 as a Delaware nonstock nonprofit corporation — stewards the proof for durable public benefit, with purposeful proliferation and global adoption paramount. The legacy is Vernam and Shannon, completed by McGough. **Security, Settled.**

Paul worked alone on this problem for thirty years. **In March 2026 the proof closed. The public release followed on June 1, 2026 — the formal paper in the public record, the reference implementation on GitHub, the stewardship in the Enqpy™ Foundation.**

Paul McGough · Founder, NQP LLC · Inventor, Enqpy™ · RPM@enqpy.com
enqpy.com · github.com/nqp-llc/enqpy · PCT/US26/22552

© 2026 NQP LLC • enqpy.com